PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 00/07330

(43) International Publication Date: 10 February 2000 (10.02.00)

(21) International Application Number: PCT/US99/16909

(22) International Filing Date: 27 July 1999 (27.07.99)

(30) Priority Data:
09/123,793 28 July 1998 (28.07.98) US

(71) Applicant: COMMERICAL ELECTRONICS, LLC [US/US]; Suite 1604, 375 Park Avenue, New York, NY 10152 (US).

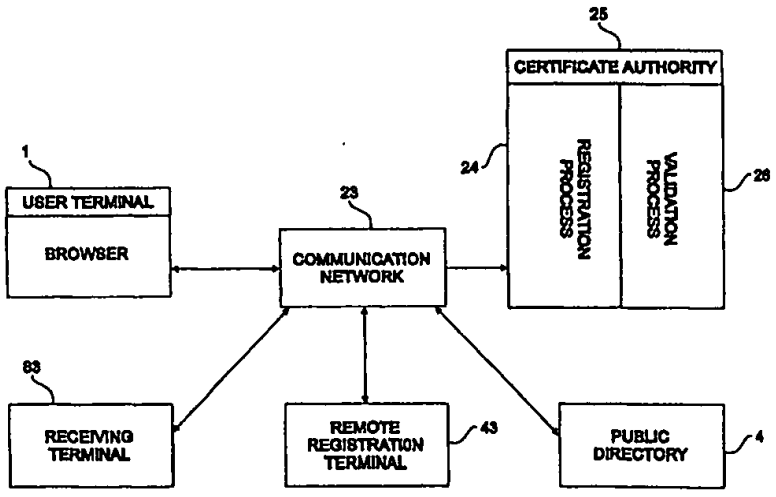
(72) Inventors: PADGETT, Robert, D.; 9519 Orion Court, Burke, VA 22015 (US). MAXWELL, John, C., III; Commerical Electronics, LLC, Suite 1604, 375 Park Avenue, New York, NY 10152 (US).

(74) Agent: LIEB, Stephen, J.; Orrick, Herrington & Sutcliffe LLP, 666 Fifth Avenue, New York, NY 10103 (US).

(81) Designated States: CA, IL, JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: DIGITAL SIGNATURE PROVIDING NON-REPUDIATION BASED ON BIOLOGICAL INDICIA



(57) Abstract

A digital certificate is formed in a terminal (1) from a digitized representation of a unique biological feature of a registrant. The digital representation is signed with the registrant's private encryption key in the terminal (1) and transmitted to a certificate authority (25) through a communication network (23). The registrant's identity is verified at a remote registration terminal (43). After identity verification, the certificate authority forms the certificate by encrypting the digital signature with the certificate authority's own encrypting key in the registration process (24). The certificate is also held in a publicly available directory (4). The document and the certificate are then transmitted to a receiving terminal (83). If the sending party denies sending the document, the biological feature can be extracted from the certificate and directly compared with the actual biological feature of the sending party in the validation process (26).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Title: DIGITAL SIGNATURE PROVIDING NON-REPUDIATION BASED ON BIOLOGICAL INDICIA

FIELD OF THE INVENTION

The present invention relates generally to the field of authentication of electronic documents, and more particularly to a non-reputable digital signature that allows authentication of the identity of the sender of a message by comparison with the sender's unique biological indicia.

BACKGROUND

Electronic commerce is rapidly becoming a ubiquitous means of conducting business. The growing popularity of the Internet and World Wide Web has opened new avenues for the conduct of business. Execution of complicated business transactions electronically present a number legal and financial problems.

Security of electronic transactions is an area of concern because messages transmitted across public networks can be intercepted. A number of encryption methods have been developed which allow a message to be read only by the designated receiver. Using so-called public key encryption, party A sending a message to party B first encrypts the message using B's public key. B's public key can be freely distributed to anyone B wishes to communicate with. Only B's private key can decrypt the message. B keeps his private key secret and uses it to decode the message. If the message is intercepted it cannot be decoded without B's private key.

The identity of a party transmitting a message executing an electronic transaction is also of concern, particularly where one of the parties is obliged to perform in the future or is subject to some future liability. In such transactions it is necessary that the parties not be able to repudiate the agreement. Also, the identity of the parties must be clearly established so that each can be assured that the other party is in fact the person it represents to be, and is able to perform. Further, the identity of the parties may need to be established with a high degree of certainty to support a legal claim, should one of the parties later attempt to avoid or repudiate the transaction.

Digital signatures have been developed to provide a means for identifying a party transmitting an electronic message. One method for creating digital signatures is to generate public and private key pairs for each of a group of parties that may wish to exchange digitally signed documents. Each of the parties stores its public decrypting keys in a registry along with identifying information, such as the key owner's name and e-mail address. The key owners each keep their private encrypting keys secret.

To create a digital signature a party encrypts a message with his private encrypting key that includes the same identifying information that is stored in the registry. The party receiving the encrypted message goes to the registry and retrieves the sending party's public decrypting key and identifying information. The receiving party decrypts the message using the decrypting key from the registry and extracts the identifying information. If the identifying information found in the message matches the information stored in the registry then the receiving party concludes that the message is genuine. Further, there is some assurance that the sending party will not deny that he sent the message since only the sending party's private encrypting key can create a message that the sending party's public decrypting key can decode. A discussion of known digital signature techniques may be found, for example, in Meyer, Carl H. and Matyas, Stephen M., *Cryptography*, Chapter 9, pp. 386-427, John Wiley & Sons, 1982.

Known digital signature techniques suffer from certain problems. A third party may intercept a signed message and use the signed message to spoof another party. By retransmitting the signed message, the interceptor may be able to convince a recipient that he is the true sender. This is the so-called "man-in-the-middle" attack.

In addition, known digital signatures are subject to repudiation. A party may no longer wish to be bound by a disadvantageous agreement or may be subject to criminal or civil liability if he made the agreement. That party may simply deny sending a particular message. The party may claim that he did not intend to execute a transaction with a particular party but was instead the victim of a man-in-the-middle attack.

With known digital signature techniques, the only information connecting the sender with the message is the database entry in the registry containing his public decrypting key and the identifying information. Thus, the sender may repudiate a transaction by claiming that his public decrypting key was registered without his authority.

SUMMARY OF THE INVENTION

The present invention is directed to methods and apparatus for forming a digital certificate that provides positive user authentication and non-repudiation. It is an object of the present invention to provide a digital certificate for authenticating electronically transmitted documents which incorporates a unique characteristic of the sender, such as biological indicia that can only have come from the sender himself.

Another object of the present invention is to provide a digital certificate that allows positive identification of the sender which cannot be repudiated.

Yet another object of the present invention is to provide for encrypting an electronic message using a digital certificate based on biological indicia.

Yet another object of the present invention is to provide a method for positively identifying the sender of an electronic message signed with a biologically-based digital certificate.

Broadly, the present invention is directed to methods and apparatus for creating a digital certificate for use in electronic commerce which is based on biological indicia of the person providing the digital certificate such that the digital certificate provides positive identification of the sender and minimizes the ability of the sender to repudiate the authenticity of the certificate and any transaction embodied in an electronic document appended to the certificate.

According to a first aspect of the present invention there is provided a user terminal, a certificate authority, and a remote registration terminal. A person, hereinafter called a registrant, wishing to obtain a digital certificate enters a data corresponding to a biological or physical characteristic of himself, for example, his chromosomal DNA, into a terminal. Preferably, the data is entered in digital form, but could be entered by optical imaging (e.g. a photograph or a scanned fingerprint, iris, or retina) which is then processed into digital form. The digital representation of the registrant's biological indicia is encrypted using the registrant's private key and sent to the certificate authority along with the registrant's public key. The certificate authority decrypts the digital representation and stores it. The registrant then visits a remote registration terminal in person with the digital representation and other identifying documents. The operator of the remote registration terminal verifies the identity of the registrant from the identifying documents and transmits the digitized representation to the certificate authority. The certificate authority compares the decrypted digital representation with the representation sent from the remote registration terminal. If a match

is found, the certificate authority forms a certificate by signing the digital signature using the certificate authority's encrypting key. The certificate is stored in a database and is sent to the registrant. Preferably, the database is public with no restriction as to who may access the stored certificate data. Alternatively, access to the database may be restricted to, for example, employees of a particular corporation or government department, database subscribers, or members of a stock exchange.

According to another aspect of the present invention, the registrant transmits a digital message including the certificate described above. The digital message is then encrypted with the registrant's private encrypting key. The party receiving the encrypted message decrypts the message using the registrant's public decrypting key. The receiving party inspects the message to verify that the appended certificate is valid and that the certificate was prepared by a reputable certificate authority by comparing the certificate with the information stored in the database. The reputation of the certificate authority provides some assurance that the message is genuine and that the sender will not later repudiate the message because his signature and identifying information are part of the certificate stored in the public database.

If additional assurance that the registrant actually transmitted the message is desired, the receiving party can transmit the certificate to the certificate authority and request that the certificate be decrypted to extract the digitized representation. The digital representation is then compared with the digital representation originally submitted by the registrant. If even greater assurance is required, for example, where the registrant later attempts to repudiate the message, the digital representation can be compared with biological indicia of the registrant from which the digital signature was originally formed.

BRIEF DESCRIPTION OF THE DRAWINGS

Further characteristics, features, and advantages of the present invention will be apparent upon consideration of the following detailed description of the present invention, taken in conjunction with the following drawings, in which like reference characters refer to like parts, and in which:

Fig. 1 is a block diagram of a terminal used for forming a digital certificate according to a first embodiment of the present invention;

Fig. 2 is a block diagram showing components connected by a communication network for forming a digital certificate according to the first embodiment;

Fig. 3 is a block diagram showing the components of a registration process of a certificate authority used for forming a digital certificate according to the first embodiment;

Fig. 4 is a block diagram showing a remote registration terminal for forming a digital certificate according to the first embodiment;

Fig. 5 is a block diagram showing the certification process of the certificate authority for forming a certificate according to the first embodiment;

Fig. 6 is a block diagram showing a terminal used for signing an electronic message with a digital certificate according to a second embodiment of the present invention;

Fig. 7 is a block diagram showing a portion of a terminal for receiving and authenticating the electronic message signed with the digital certificate by the apparatus of Fig. 6 according to the second embodiment;

Fig. 8 is a block diagram showing a validation process according to the second embodiment;

Fig. 9 is a block diagram showing a digital key entry system according to a third embodiment of the present invention.

DETAILED DESCRIPTION

With reference to Figs. 1-5, a process for forming a digital certificate according to a first embodiment of the present invention will be described. A person wishing to obtain a certificate, hereinafter called the registrant, first visits a service provider to obtain a digitized representation of a biological characteristic of his or her body. This digitized characteristic will be referred to as a bio-blob. A bio-blob may be formed from, for example, a digitized image of the registrant's fingerprint, iris or retina or a digital representation of a marker plate prepared from the registrant's chromosomal DNA. Other physical characteristics may be used, depending on the degree of security desired. For example, an image of the registrant's footprint, handprint, dental x-ray or other distinguishing characteristic of the registrant's body may be used. The bio-blob may also be a combination of digitized images and other identifying indicia of the registrant and may include, for example, a password such as an alphanumeric string. The service provider may be a medical clinic equipped to handle and analyze biological samples.

The service provider gives the registrant the bio-blob in digital form. The bio-blob may be provided on any of a number of digital media including a magnetic tape or disk, an optical disk, or a digital memory. A preferred medium for storing the bio-blob is a non-

volatile solid-state memory incorporated in a so-called smart card for convenience and portability.

Note that in the figures "cylinders" illustrate data elements and "boxes" illustrate process functions. The data elements may be stored, for example, on magnetic or optical disk drives or in solid state memory devices. The process functions may be implemented by a general-purpose computer, for example, a personal computer, workstation, or mainframe computer, under the control of a software program. The functions described herein may also be performed by special purpose computing devices designed to perform specific data processing tasks, or by a combination of general purpose and special purpose processors.

Fig. 1 shows a terminal 1 owned by or associated with the registrant. Alternatively, the terminal 1 may be a device owned by a third party which is provided for the registrant's exclusive use in a manner explained below. The terminal 1 may be, for example, a computer workstation. The terminal 1 is connected with a reader 3. A data 2 containing the bio-blob 5 produced by the service provider is inserted into the reader 3 and the bio-blob data 5 is transferred to the terminal 1. The data 2 is preferably a smart card and the reader 3 is preferably a smart card reader, each of which is conventional in design and use.

A hash function 7 receives the bio-blob data 5 and calculates a hashed bio-blob 9. The hashed bio-blob 9 is a fixed length string which is a compressed version of the original bio-blob data 5. The hash function 7 is selected so that the bio-blob 5 is efficiently converted to the hashed bio-blob 9, but it is infeasible to generate a bio-blob that hashes to a given value. If the integrity of the hashed bio-blob 9 is violated, because of transmission errors or intentional manipulation, a receiving device can detect the violation using known error detection techniques.

A public/private key function 11 calculates a private 13 and public 15 key pair for the registrant. The key pair 13, 15 is designed to function with a so-called public-key algorithm. Messages encrypted with the private key 13 may be decrypted with the public key 15. However, knowledge of the public key 15 does not allow efficient calculation of the private key 13. For example, the key pair 13, 15 may be generated to work in the so-called RSA algorithm.

The hashed bio-blob 9 and the private key 13 are received by the signature function 17. The signature function 17 signs the hashed bio-blob 9 by encrypting it with the private key 13 to generate the signature 19. The registrant enters identifying information into a registration form 16. The registration form 16 is an electronic document which queries the

registrant for identifying information such as the registrant's name, social security number, mother's maiden name, address, and telephone number. The registration form 16 may be a so-called Hypertext Mark-up Language (HTML) page.

The public key 15 is combined with the registration form 16 to create a message 18. The message 18 and the signature 19 are formatted by the browser function 21 for transmission across a communication network 23 via a modem 22. The modem 22 formats the transmitted signal in a form which is compatible with the communication network. The communication network 23 may be, for example, an intranet, an internet or an extranet. The communication network 23 may be implemented, for example, using a public data network (PDN) or a private communication link, such as wide area network, a local area network, or a dedicated telephone line. The communication network 23 allows communication between and among the terminal 1, a public directory 4, a certificate authority 25, a registration manager 43, and a receiving terminal 83. The certificate authority 25 includes a registration process 24 and a validation process 26. Fig. 2 shows the registrant's terminal 1 connected with the communication network 23.

The message 18 and signature 19 are transmitted from the terminal 1 to the certificate authority 25. Fig. 3 shows the registration process 24 of the certificate authority 25 in detail. Digital signals are received from the communication network 23 by the modem 28 which sends the message 18 and signature 19 to the user input registration process 27. The user input registration process 27 parses the message 18 and signature 19 from the communication network 23. The public key 15, registration form 16, and signature 19 are stored in the input queue 29. The decryption process 31 retrieves the signature 19 and public key 15 from the input queue 29. The decryption process 31 decrypts the signature 19 using the public key 15 to recover the hashed bio-blob 9. The hashed bio-blob 9 is then de-hashed by the de-hashing function 33 to recover the bio-blob 5. The bio-blob 5 is stored as a flat file in the bio-blob queue 35.

The compare function 37 retrieves the bio-blob 5 from the bio-blob queue 35 and compares it with bio-blobs stored in the registered bio-blob database 39. The registered bio-blob database 39 contains bio-blobs from persons who have completed the registration process, as will be described later. Because the registrant has not yet completed the registration process, no match will be found by the compare function 37. The compare function 37 sends a command to the rejection process 41 which sends a message to the

terminal 1 via the communication network 23 instructing the registrant to complete the registration process. The bio-blob 5 remains in the bio-blob queue 35.

The registrant goes to a remote registration terminal 43 with the smart card 2 containing the digitized bio-blob 5 and physical identification which confirm the information entered in the registration form 16. The physical identification may be, for example, the registrants driver's license, passport, or other government-issued identification card. Preferably, the physical identification includes a photograph of the registrant. The remote registration terminal 43 is located at a service provider and the registrant must be physically present to be registered. An operator at the remote registration terminal 43 enters identifying information from the physical identification into a verification form 18. The verification form 18 may be an HTML page which queries the operator of the remote registration terminal for the same information requested by the registration form 16.

Fig. 4 shows the remote registration terminal 43 in detail. The bio-blob 5 stored on the smart card 2 is read by a reader 45 and sent to the registration input process 47. The operator enters information to the verification form 18 using an input device 49. The input device 49 may be a keyboard or a pointing device coupled to a graphical user interface. The registration input process 47 combines the bio-blob 5 with the verification form 18 to generate a registration request 51. The registration request 51 is formatted by the communication manager 53, transmitted by the modem 54 and sent to the registration process 24 of the certificate authority 25 across the communication network 23.

Referring again to Fig. 3, modem 28 receives the registration request 51 and sends it to the registration manager input process 55. The registration request 51 is stored in the registration queue 57. The registration process 59 retrieves the registration request 51 from the registration queue 57 and extracts the bio-blob 5. The bio-blob 5 is stored in the registered bio-blob database 39 along with the verification form 18.

The compare function 37 compares each newly registered bio-blob in the registered bio-blob database 39 with the bio-blobs stored in the bio-blob queue 35. When the registrant's bio-blob 5 is found in both the bio-blob queue 35 and registered bio-blob database 39, the compare function 37 sends a message to the certification process 61 indicating that a match has been found. The compare function 37 also compares the registration form 16 with the verification form 18 submitted from the remote registration terminal 43 to verify the identity of the registrant.

The certification process 61 is shown in detail in Fig. 5. When a message is received from the compare function 37 indicating a match between the bio-blob queue 35 and the registered bio-blob database 39, the registration form 16, public key 15, and signature 19 are retrieved from the input queue 29. A key function 63 generates a certificate signing key 65 and a certificate public key 67. The certification process 69 encrypts the signature 19 using the certificate authority's signing key 65. The encryption process 69 appends certificate authority identity information 70 to the encrypted signature 19. The identity information 70 may be contained on an HTML page capable of supporting active links across the communication network 23. The encrypted signature 19 and identity information 70 form the certificate 71. The certificate 71 is sent to the registrant's terminal 1 via the communication network 23. The certificate 71 is also stored in certificate archive 73 along with the certificate authority's public key 67.

The certificate 71 is sent to a public directory 4 via the communication network 23. According to a preferred embodiment, any terminal connected to the communication network 23 may read the public directory 4. Alternatively, access to the directory 4 may be limited to certain authorized persons. The public directory 4 contains all the valid certificates for each registrant on the communication network 23. The public directory 4 also contains a list of certificates that are no longer valid. Parties can compare certificates received with electronic documents against the certificates stored in the public directory 4 via the communication network 23 to determine if a document includes a valid certificate. The identity information 70 in each certificate may include an active link to the public directory 4 allowing a party to access the valid certificates and list of invalid certificates conveniently.

There is an advantage in having the digital signature 19 prepared at the registrant's terminal 1 and then having the registrant register in person at the remote registration terminal 43 using his bio-blob 5. The registrant maintains control over the key pair 13, 15 , as well as his bio-blob 5 stored on the smart card 2, which were used to prepare the signature 19 that forms the basis for the certificate 71. The registrant cannot later claim that a certificate 71 was prepared without his authorization.

If the key pair 13, 15 or the smart card 2 are disclosed to others, the registrant must inform the public directory 4 to add the certificate 71 to the list of invalid certificates. A new certificate will have to be prepared. If another party receives an electronic document signed using the now invalid certificate, that party will know that the document cannot be relied upon.

Figs. 6, 7, and 8 show an apparatus for sending signed electronic messages via the communication network 23 according to a second embodiment of the present invention. Fig. 6 shows the process of sending a message from the registrant's terminal 1 using the certificate 71. A transaction message 75 is formed including, for example, a contract the user wishes to execute with the operator of the receiving terminal 83. The encryption process 77 joins the transaction message 75 with the certificate 71 and encrypts the result using the registrant's private key 13 to form the signed message 79. The signed message 79 is transmitted by the modem 80 and sent via the communication network 23 to a receiving terminal 83.

Fig. 7 shows the authentication of the signed message 79 by the receiving terminal 83. The signed message 79 is received by the modem 76 and is decrypted by the decryption process 85 using the registrant's public key 15 thereby recovering the transaction message 75 and the certificate 71. An authentication process 87 inspects the identity information 70 which is part of the certificate 71. The authentication process 87 accesses the public directory 4 via the communication network 23 to verify that the certificate 71 is valid. According to a preferred embodiment an active link to the public directory 4 embedded in the identity information 70 simplifies this process. For transactions where there is little risk that a message is fraudulent, simply verifying that the sender has a valid certificate 71 from a reputable certificate authority 25 is sufficient to proceed with the transaction.

An additional level of security can be obtained by recovering the bio-blob 5 from the certificate 71 and comparing it with the bio-blob 5 encrypted within the certificate 71 stored in the public directory 4. Fig. 8 shows a validation process 26 performed by the certificate authority 25. The certificate authority public key 67 is retrieved from the certificate archive 73 and is used by the decryption process 72 to decrypt the certificate 71 to extract the digital signature 19. The registrant's public key 15 is then used by the decryption process 74 to decrypt the signature 19 to extract the hashed bio-blob 9. The hashed bio-blob 9 is dehashed by the dehash process 76 to extract the bio-blob 5. The compare function 37 retrieves the bio-blob 5 that was stored in the registered bio-blob database 39 during the registration process and compares it with the bio-blob 5 extracted from the certificate 71.

The identity of the person sending the message may be positively confirmed by comparing the bio-blob 5 extracted from the certificate 71 to an actual biological feature of the person alleged to have sent the message. For example, if the bio-blob 5 were a digital representation of a DNA marker plate prepared from the registrant's tissue, then a similar marker plate could be prepared from tissue taken from the alleged sender's body. If the bio-

blob 5 matches the alleged sender's marker plate then it is virtually certain that the sender is the registrant.

The digital certificate 71 described above may be used to authenticate electronic document 75 transmitted between remote parties via a communication network 23. However, the invention is not limited to this type of communication. The digital certificate 71 according to the present invention is applicable to any type of digital message where non-repudiation and positive identification are required. Fig. 9 illustrates a third embodiment of the present invention where the digital certificate 71, formed according to the first embodiment, is incorporated into a key access card 91 to be used, for example, by an employee to gain access to a restricted area of an employer's building. The digital certificate 71 is stored in a memory on the card 91 along with conventional identifying information such as the employee's name 92. The memory may be a solid-state device, a magnetic strip, a pattern of marks or another known technique for storing digital data. The registrant, for example, an employee seeking access to a restricted area, presents the card 91 to a card reader 93. The reader 93 retrieves the certificate 71 and name 92 from the card 91 and communicates them to a processor 97 via an internal network 95. The processor 97 compares the certificate 71 with a database of valid certificates 101 and if a match is found, the employee is allowed access. The employee name 92 and certificate 71 are stored in an access database 99 by the processor 97. Routine reports of access activity can be generated based on the employee name 92 alone. If positive proof that a particular employee entered the restricted area, for example where a crime has been committed, the digital certificate 71 can be retrieved from the access database 99 and the bio-blob 5 encoded therein can be compared with the biological indicia of the employee.

The above embodiments are illustrative of the present invention. While these are presently considered the most practical and preferred embodiments, it is to be understood that the invention is not limited by this disclosure. This invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the invention, as will be apparent to a person of ordinary skill in the art.

We claim:

1. A digital certificate comprising:

a digitized biological indicium encrypted with a first encrypting key and encrypted with a second encrypting key, the second encrypting key being generated by a certificate authority; and

certificate authority identity information, wherein the biological indicium uniquely identifies a registrant.

2. The certificate according to claim 1 wherein the first encrypting key is generated at a terminal remote from the certificate authority, the terminal being associated with the registrant.

3. The certificate according to claim 1 wherein the certificate authority identity information includes an active link to a registry of valid certificates.

4. The certificate according to claim 3 wherein the registry further comprises a list of invalid certificates.

5. An electronic document comprising:

message information and a digital certificate, wherein the digital certificate includes a digitized biological indicium, the biological indicium uniquely identifying a registrant.

6. The document according to claim 5 wherein the digital certificate is stored in a database by a certificate authority.

7. The document according to claim 5 wherein the digitized biological indicium is encrypted by the registrant using a first encrypting key and encrypted by the certificate authority using a second encrypting key.

8. A data card comprising:

a memory;

information stored in the memory identifying a registrant; and

a digital certificate stored in the memory, wherein the digital certificate includes a digitized biological indicium, the biological indicium uniquely identifying the registrant.

9. The data card according to claim 8 further comprising:

a reader connected to the memory;

a certificate database containing a verified copy of the digital certificate;

an access database; and

a processor connected to the reader, the certificate database and the access database, wherein the processor commands the reader to read the digital certificate and the identifying information from the memory, compares the digital certificate from the memory with the verified copy in the certificate database and stores the identifying information in the access database.

10. A method for forming a certificate for authentication of electronic messages, the method comprising:

providing a digital representation of a biological indicium of a registrant;

first encrypting the digital representation to form a digital signature;

transmitting the digital signature to a certificate authority; and

second encrypting the digital signature by the certificate authority to form the certificate.

11. The method according to claim 10 further comprising hashing the digital representation prior to the step of first encrypting.

12. The method according to claim 10 further comprising providing the biological indicium as an optical image.

13. The method according to claim 12 further comprising providing the optical image as an image of a fingerprint of the registrant.

14. The method according to claim 12 further comprising providing the optical image as an image of an iris of an eye of the registrant.

15. The method according to claim 12 further comprising providing the optical image as an image of the retina of an eye of the registrant.

16. The method according to claim 10 further comprising providing the biological indicium as a feature of a biochemical substance extracted from a tissue sample of the registrant.

17. The method according to claim 16 wherein the biochemical substance includes chromosomal deoxyribonucleic acid.

18. The method according to claim 10 wherein the step of first encrypting comprises forming a first encrypting key according to a public key algorithm and encrypting the digitized representation using the first encrypting key, and wherein the step of second encrypting comprises forming a second encrypting key according to the public key algorithm and encrypting the signature using the second encrypting key.

19. The method according to claim 18 further comprising providing a workstation in the custody of the registrant and performing at least one of the first encrypting step and the second encrypting step at the workstation.

20. The method according to claim 10 further comprising:

entering information identifying the registrant;

appending the identifying information to the digital signature;

verifying the entered identifying information at a remote registration terminal to generate verification information; and

transmitting the verification information from the remote registration terminal to the certificate authority.

21. A certificate formed by the method of claim 10.

22. A method of authenticating an electronic document, the method comprising:

providing a digitized biological indicium of a registrant;

first encrypting the digitized biological indicium to form a digital signature;

authenticating the digital signature;

second encrypting the digital signature to form a certificate;

storing the certificate in a registry;

appending the certificate to the electronic document to form a signed document;

transmitting the signed document to a receiving terminal by an electronic transmission means;

extracting the certificate from the transmitted signed document; and

comparing the extracted certificate with the certificate stored in the registry.

23. A signed document formed by the steps of providing, first encrypting, authenticating, second encrypting, storing and appending according to the method of claim 22.

24. The method according to claim 22 wherein the step of first encrypting comprises:

forming a first private encrypting key and a first public decrypting key and encrypting the digitized biological indicium using the first private encrypting key, and wherein the step of storing the certificate comprises storing the first public decrypting key in the registry.

25. The method according to claim 22 wherein the step of authenticating comprises:

storing the digitized biological indicium on a storage medium;

transmitting the digital signature to a certificate authority from a registrant terminal;

decrypting the digital signature to extract the digitized biological indicium;

registering the registrant by entering identifying information provided by the registrant into a registration terminal;

retrieving the digitized biological indicia from the storage medium by the registration terminal;

transmitting the identifying information and the digitized biological indicium to the certificate authority from the registration terminal; and

comparing the transmitted digitized biological indicium with the digitized biological indicium extracted by the certificate authority.

26. The method according to claim 22 wherein the step of second encrypting comprises generating a second private encrypting key and a second public decrypting key by the certificate authority and encrypting the digital signature using the second private encrypting

key and wherein the step of storing the certificate comprises storing the second public decrypting key in the registry.

27. The method according to claim 26 further comprising:

retrieving the second public decrypting key from the registry;

decrypting the certificate using the second public decrypting key to obtain the digital signature;

decrypting the digital signature using the first public decrypting key to extract the digitized representation; and

comparing the extracted digitized representation with the biological indicium of the registrant.

28. The method according to claim 22 further comprising providing the biological indicium as an optical image.

29. The method according to claim 28 further comprising providing the optical image as an image of a fingerprint of the registrant.

30. The method according to claim 28 further comprising providing the optical image as an image of an iris of eye of the registrant.

31. The method according to claim 28 further comprising providing the optical image as an image of the retina of an eye of the registrant.

32. The method according to claim 22 further comprising providing the biological indicium as a feature of a biochemical substance extracted from a tissue sample of the registrant.

33. The method according to claim 32 wherein the biochemical substance includes chromosomal deoxyribonucleic acid.

34. An apparatus for forming a certificate comprising:

a storage medium containing a digital representation of a biological indicium of a registrant;

a terminal including:

input means for reading the storage medium and for inputting the digital representation;

first encrypting means for encrypting the digitized representation to form a digital signature; and

transmitting means for transmitting the digital signature; and

a certificate authority, the certificate authority including:

receiving means for receiving the transmitted digital signature;

decrypting means for decrypting the digital signature to extract the digital representation;

authenticating means for verifying that the biological indicium represented by the digital representation corresponds to the registrant; and

second encrypting means for encrypting the digital signature to form the certificate.

35. The apparatus according to claim 34 wherein the user workstation includes hashing means for hashing the digital representation.

36. The apparatus according to claim 34 wherein the transmitting means includes a communication network.

37. The apparatus according to claim 36 wherein the authenticating means includes a remote registration terminal connected with the certificate authority via the communication network.

38. The apparatus according to claim 37 wherein the remote registration terminal includes a reader for reading the digital representation from the storage medium and input means for inputting information identifying the registrant.

39. An apparatus for forming a certificate comprising:

a communication network;

a memory containing a digital representation of a biological indicium of a registrant;

a terminal including:

a reader responsive to the memory to capture the digital representation;

a first encrypting processor connected with the reader; and

a first modem connected with the first encrypting processor, wherein the first encrypting processor encrypts the digital representation retrieved from the memory to form a digital signature and causes the first modem to transmit the digital signature via the communication network; and

a certificate authority, the certificate authority including:

a second modem connected with the communication network, wherein the second modem receives the digital signature from the communication network;

a decrypting processor connected with the second modem, wherein the decrypting processor receives the digital signature from the second modem and decrypts the digital signature to recover the digital representation;

a comparator connected to the decrypting processor, wherein the comparator receives the digital representation from the decrypting processor and compares the digital representation with a verified digital signature and, if a match is found between the digital signature and the verified digital signature, the comparator generates an authenticated signal; and

a second encrypting processor connected with the comparator and responsive to the authenticated signal, wherein, in response to the authenticated signal, the second encrypting processor encrypts the digital signature thereby forming a digital certificate.

40. An apparatus for forming a certificate for authentication of electronic messages, the apparatus comprising:

a digital representation of a biological indicium of a registrant;

first encrypting means for encrypting the digital representation to form a digital signature;

data collection means for entering identifying information about the registrant;

appending means for appending the identifying information to the digital signature;

transmitting means for transmitting the digital signature to a certificate authority; and

second encrypting means for encrypting the digital signature by the certificate authority to form the certificate.

41. An apparatus for authenticating an electronic document, the apparatus comprising:

a digitized biological indicium of a registrant;

first encrypting means for encrypting the digitized biological indicium to form a digital signature;

authenticating means for authenticating the digital signature;

second encrypting means for encrypting the digital signature to form a certificate;

a memory for storing the certificate in a registry;

appending means for appending the certificate to the electronic document to form a signed document;

transmitting means for transmitting the signed document to a receiving terminal;

extracting means for extracting the certificate from the transmitted signed document; and

comparing means for comparing the extracted certificate with the certificate stored in the registry.

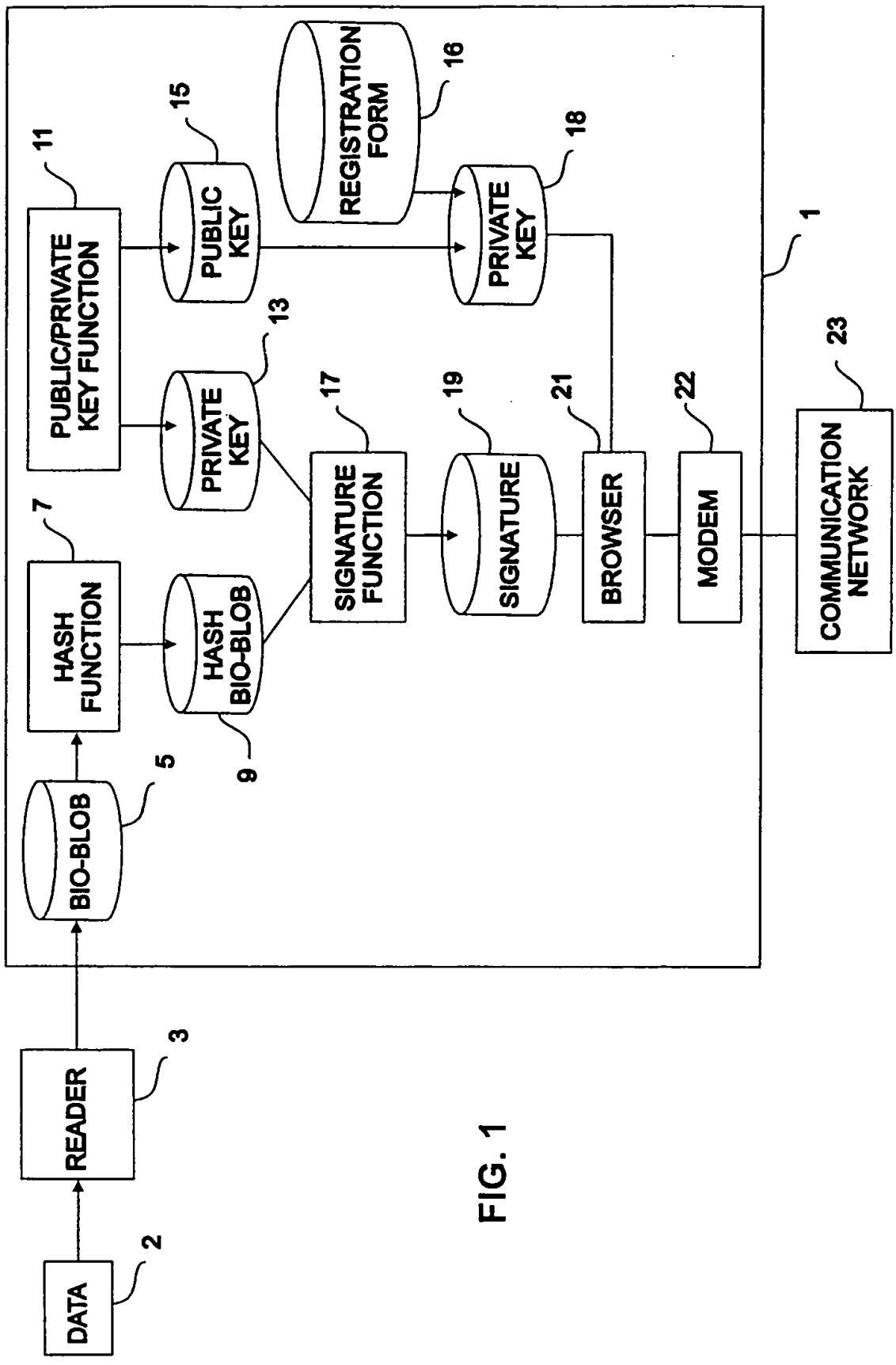

DATA
2
READER
3
BIO-BLOB
5
HASH FUNCTION
7
HASH BIO-BLOB
9
PUBLIC/PRIVATE KEY FUNCTION
11
PUBLIC KEY
15
REGISTRATION FORM
16
PRIVATE KEY
18
PRIVATE KEY
13
SIGNATURE FUNCTION
17
SIGNATURE
19
BROWSER
21
MODEM
22
COMMUNICATION NETWORK
23
1

FIG. 1

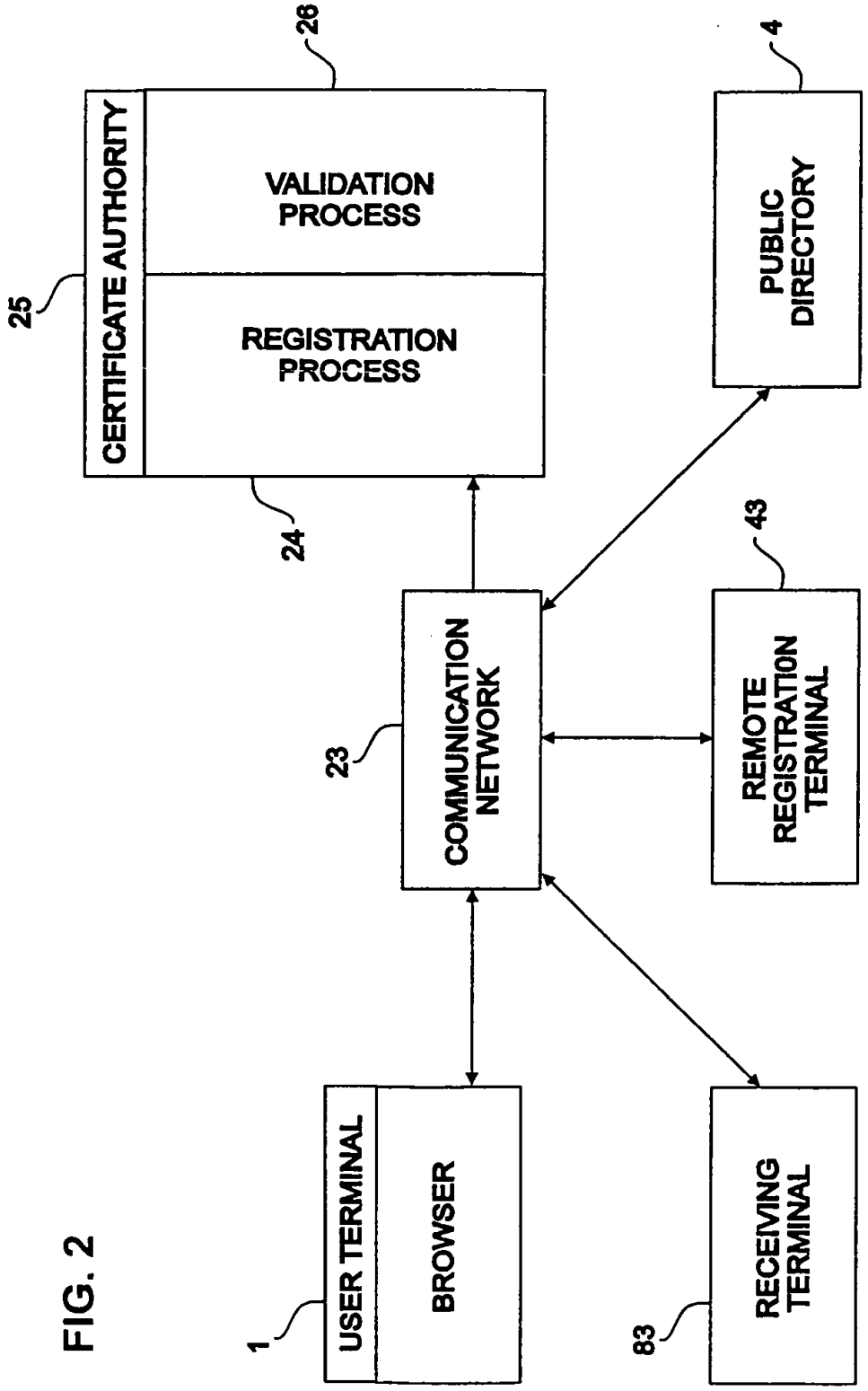

26
VALIDATION PROCESS
REGISTRATION PROCESS
CERTIFICATE AUTHORITY
25
24
4
PUBLIC DIRECTORY
43
23
COMMUNICATION NETWORK
REMOTE REGISTRATION TERMINAL
1
USER TERMINAL
BROWSER
83
RECEIVING TERMINAL

FIG. 2

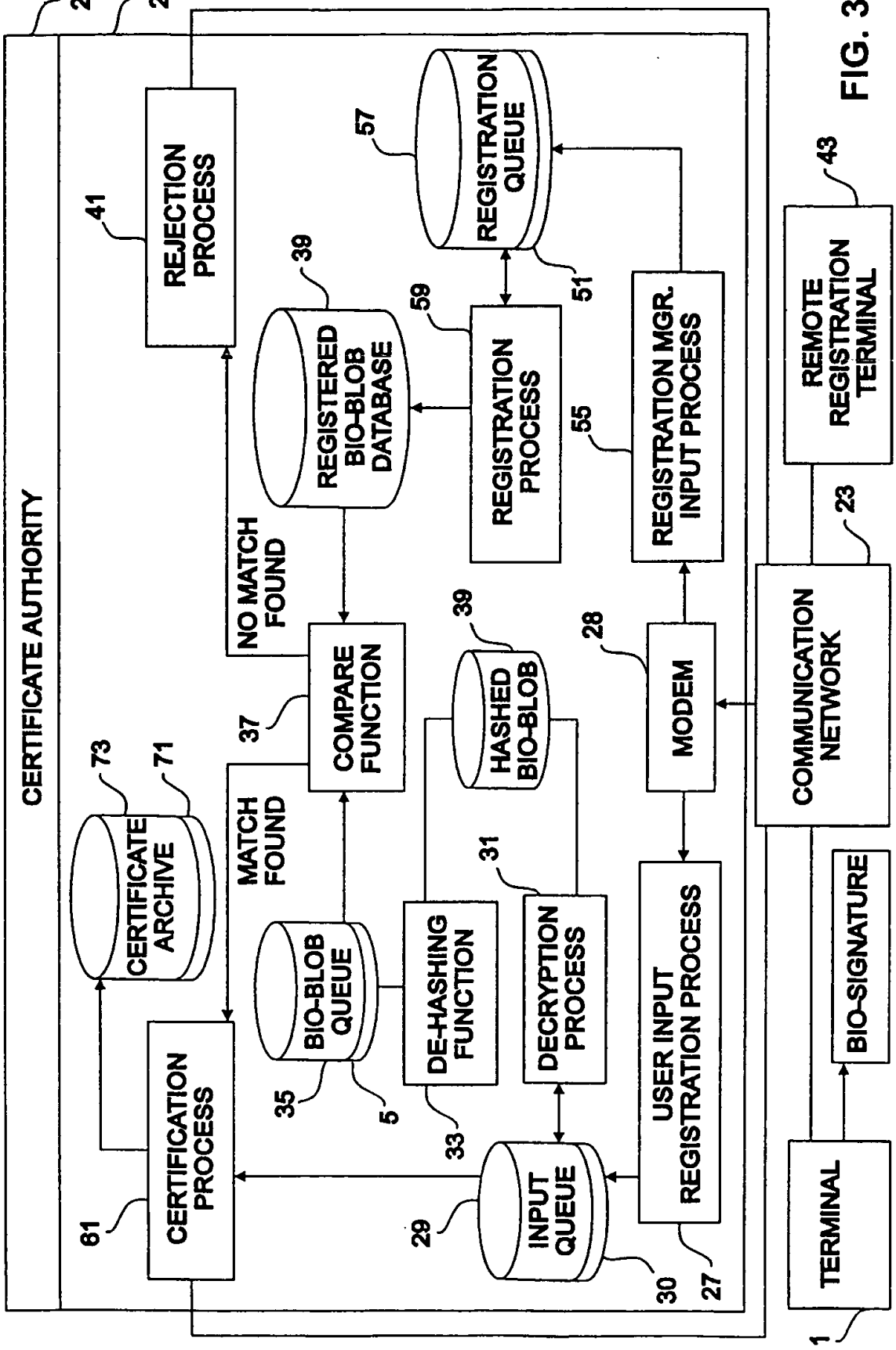

CERTIFICATE AUTHORITY
24
25
REJECTION PROCESS
41
REGISTRATION QUEUE
57
51
REGISTERED BIO-BLOB DATABASE
39
REGISTRATION PROCESS
59
REGISTRATION MGR. INPUT PROCESS
55
REMOTE REGISTRATION TERMINAL
43
NO MATCH FOUND
COMPARE FUNCTION
37
HASHED BIO-BLOB
39
MODEM
28
COMMUNICATION NETWORK
23
CERTIFICATE ARCHIVE
73
71
MATCH FOUND
BIO-BLOB QUEUE
35
5
DE-HASHING FUNCTION
DECRYPTION PROCESS
31
USER INPUT REGISTRATION PROCESS
BIO-SIGNATURE
CERTIFICATION PROCESS
61
INPUT QUEUE
29
33
30
27
TERMINAL
1

FIG. 3

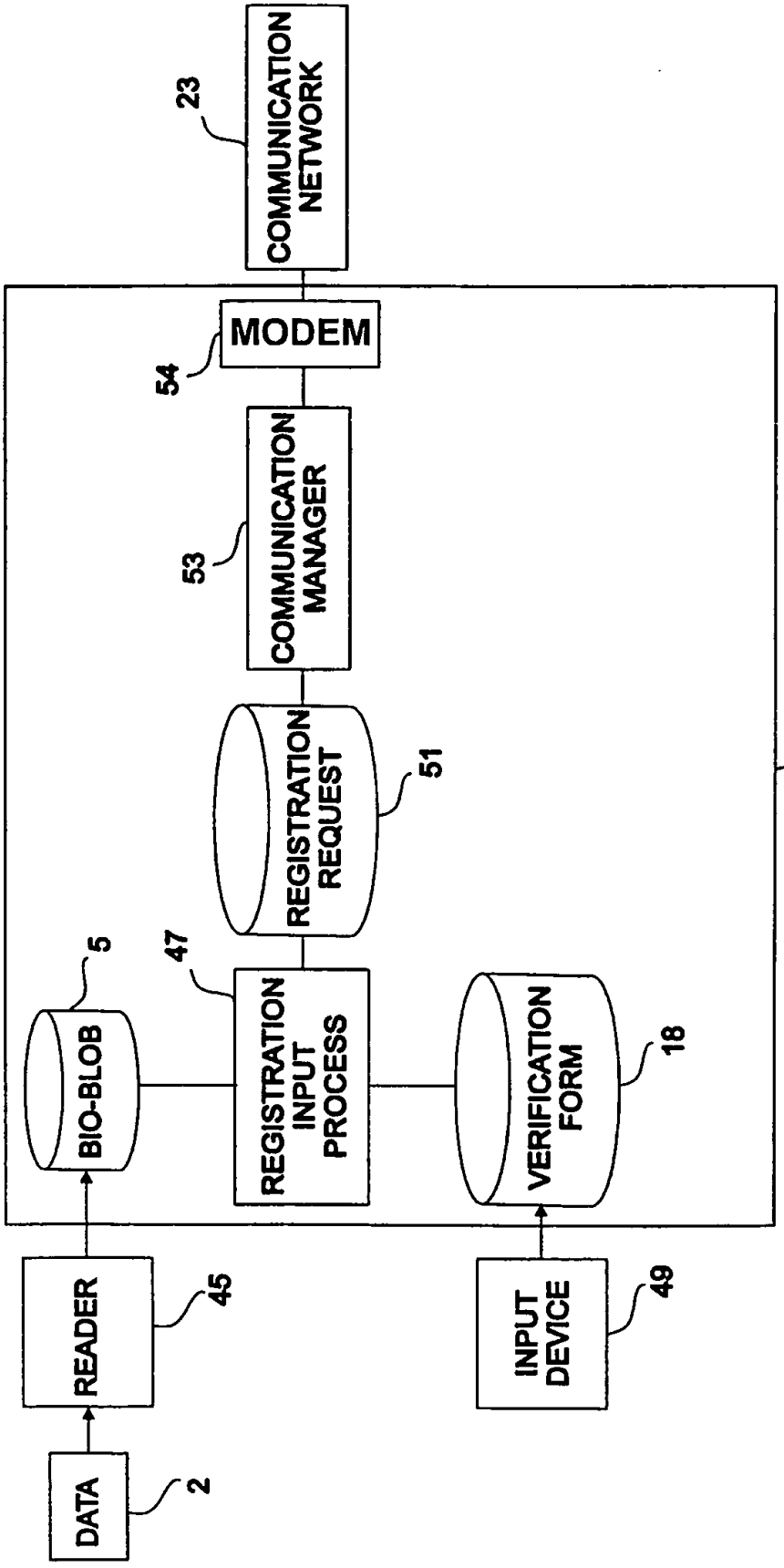

COMMUNICATION NETWORK
23
MODEM
54
COMMUNICATION MANAGER
53
REGISTRATION REQUEST
51
43
5
47
BIO-BLOB
REGISTRATION INPUT PROCESS
VERIFICATION FORM
18
READER
45
INPUT DEVICE
49
DATA
2

FIG. 4

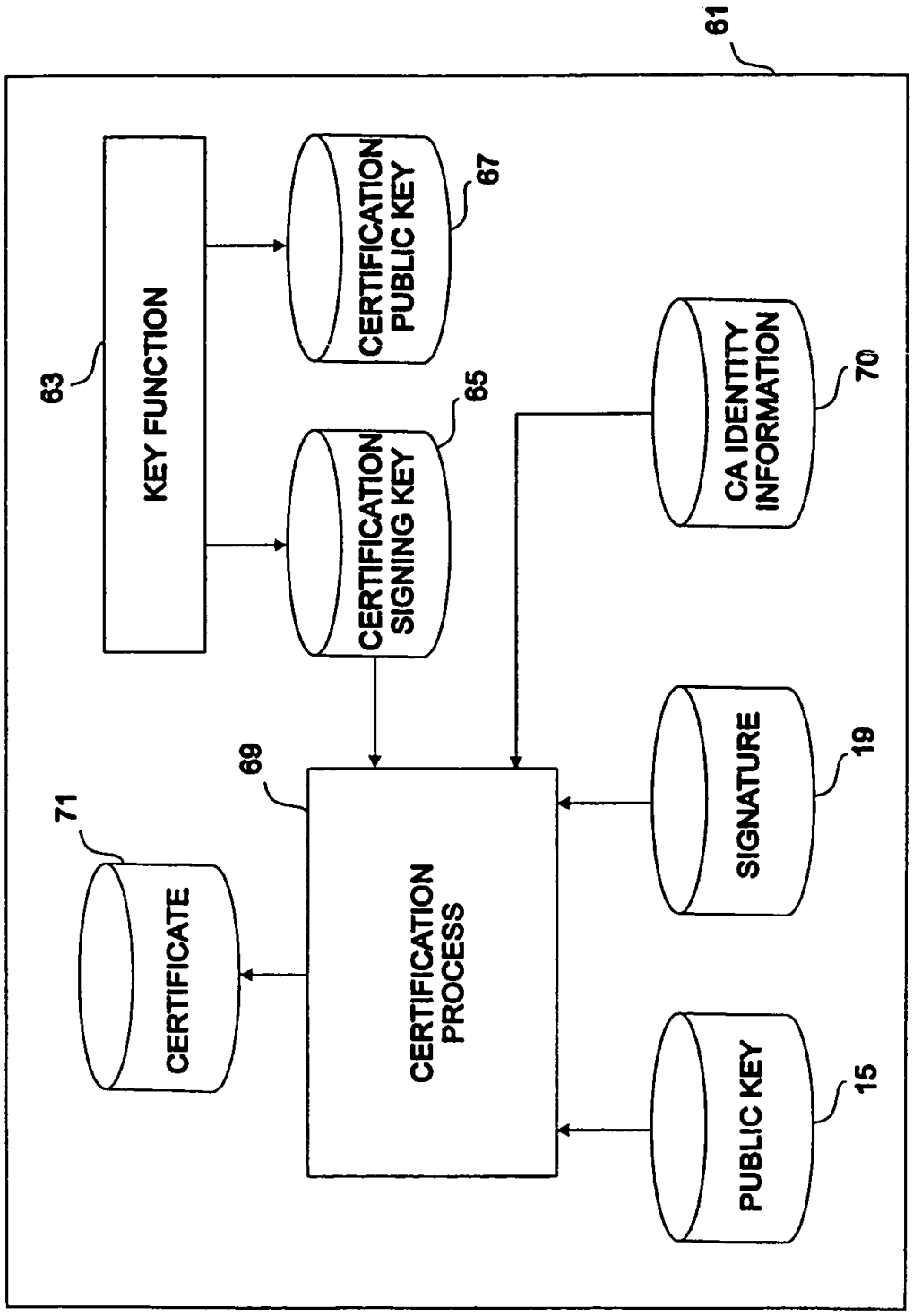
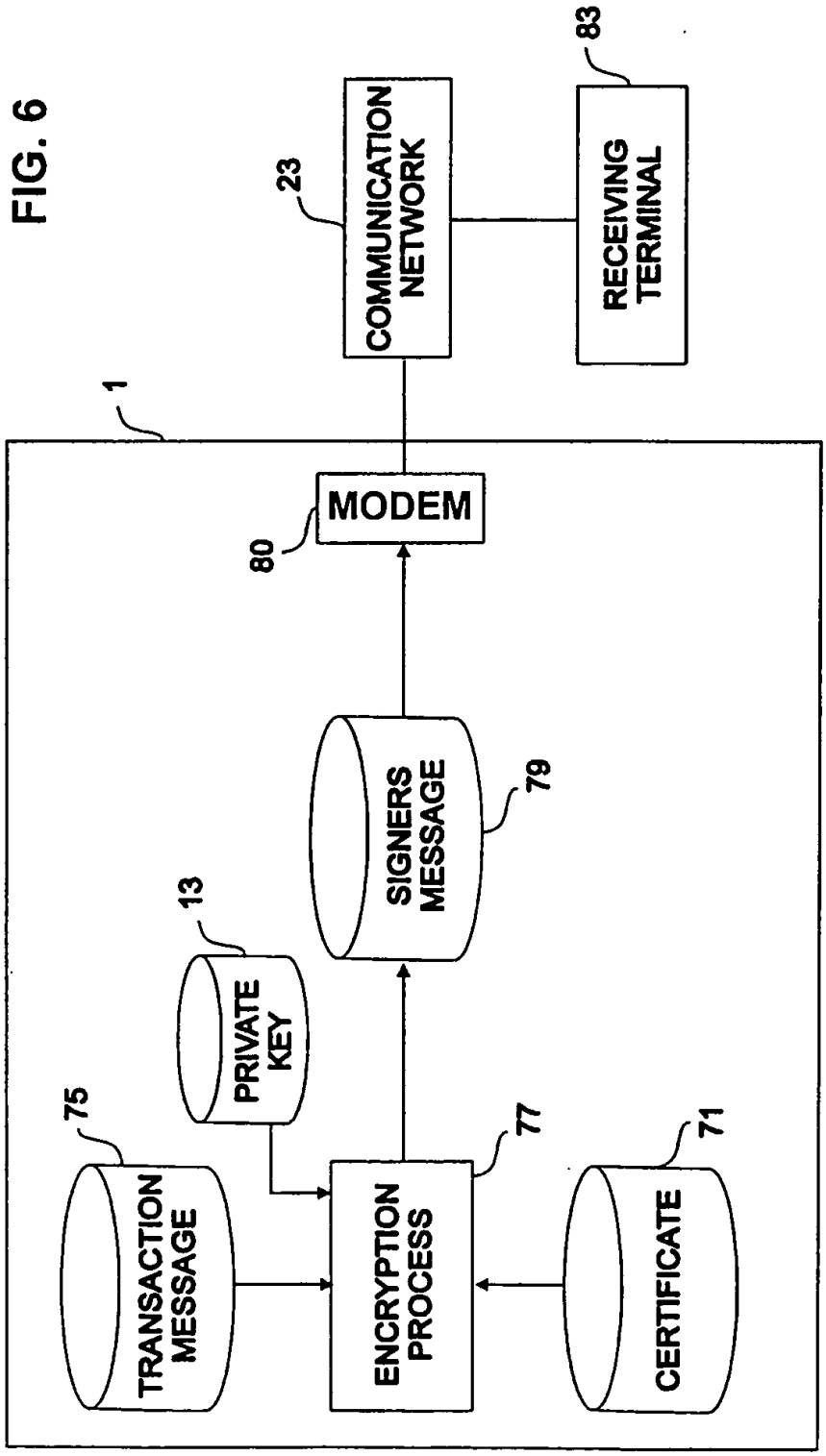

81
KEY FUNCTION
63
CERTIFICATION PUBLIC KEY
67
CERTIFICATION SIGNING KEY
65
CA IDENTITY INFORMATION
70
SIGNATURE
19
CERTIFICATION PROCESS
69
CERTIFICATE
71
PUBLIC KEY
15

FIG. 5

FIG. 6


83
RECEIVING TERMINAL
23
COMMUNICATION NETWORK
1
MODEM
80
SIGNERS MESSAGE
79
13
PRIVATE KEY
75
TRANSACTION MESSAGE
77
ENCRYPTION PROCESS
71
CERTIFICATE

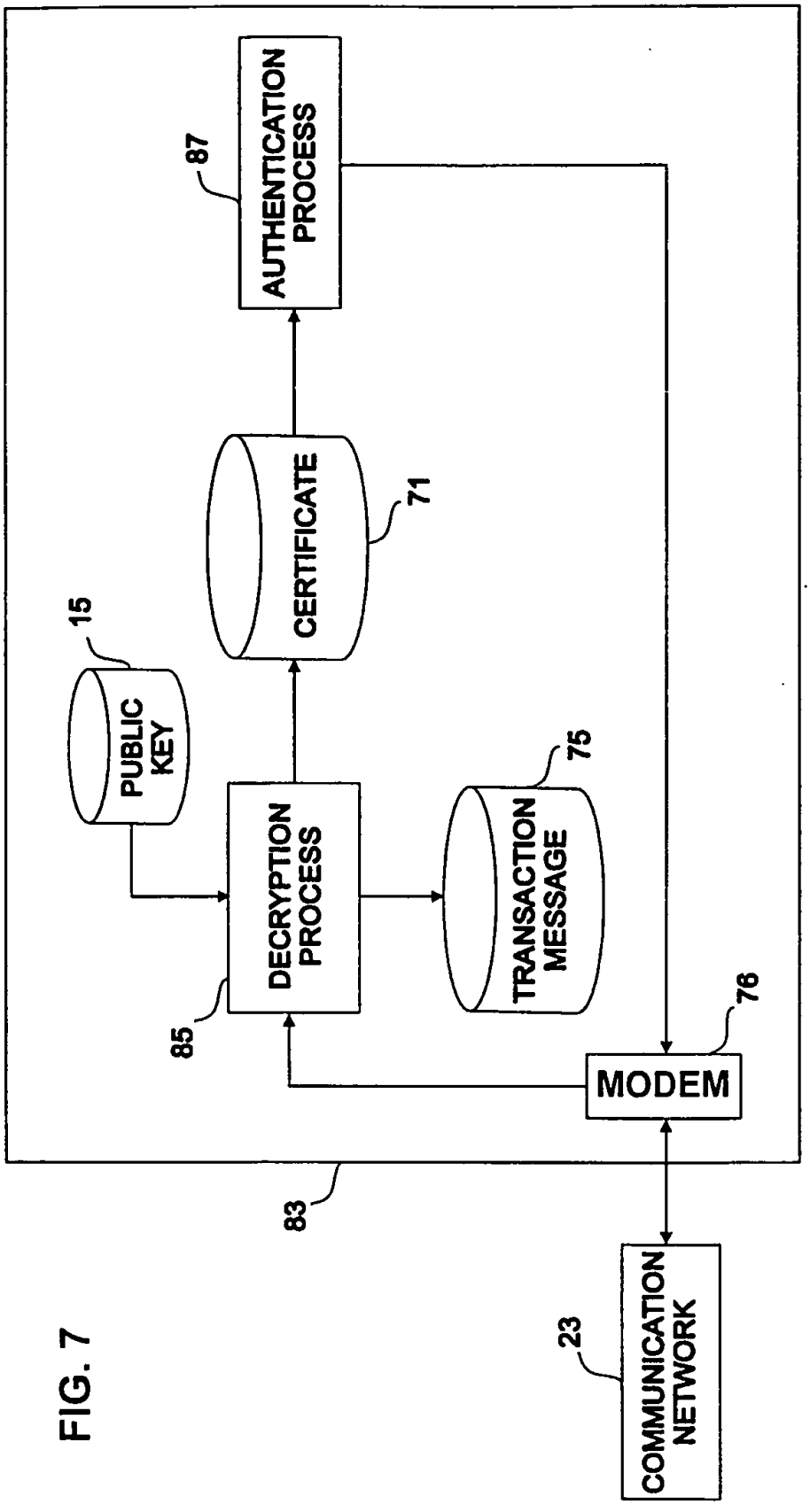

AUTHENTICATION PROCESS
87
CERTIFICATE
71
PUBLIC KEY
15
DECRYPTION PROCESS
85
TRANSACTION MESSAGE
75
MODEM
76
83
COMMUNICATION NETWORK
23

FIG. 7

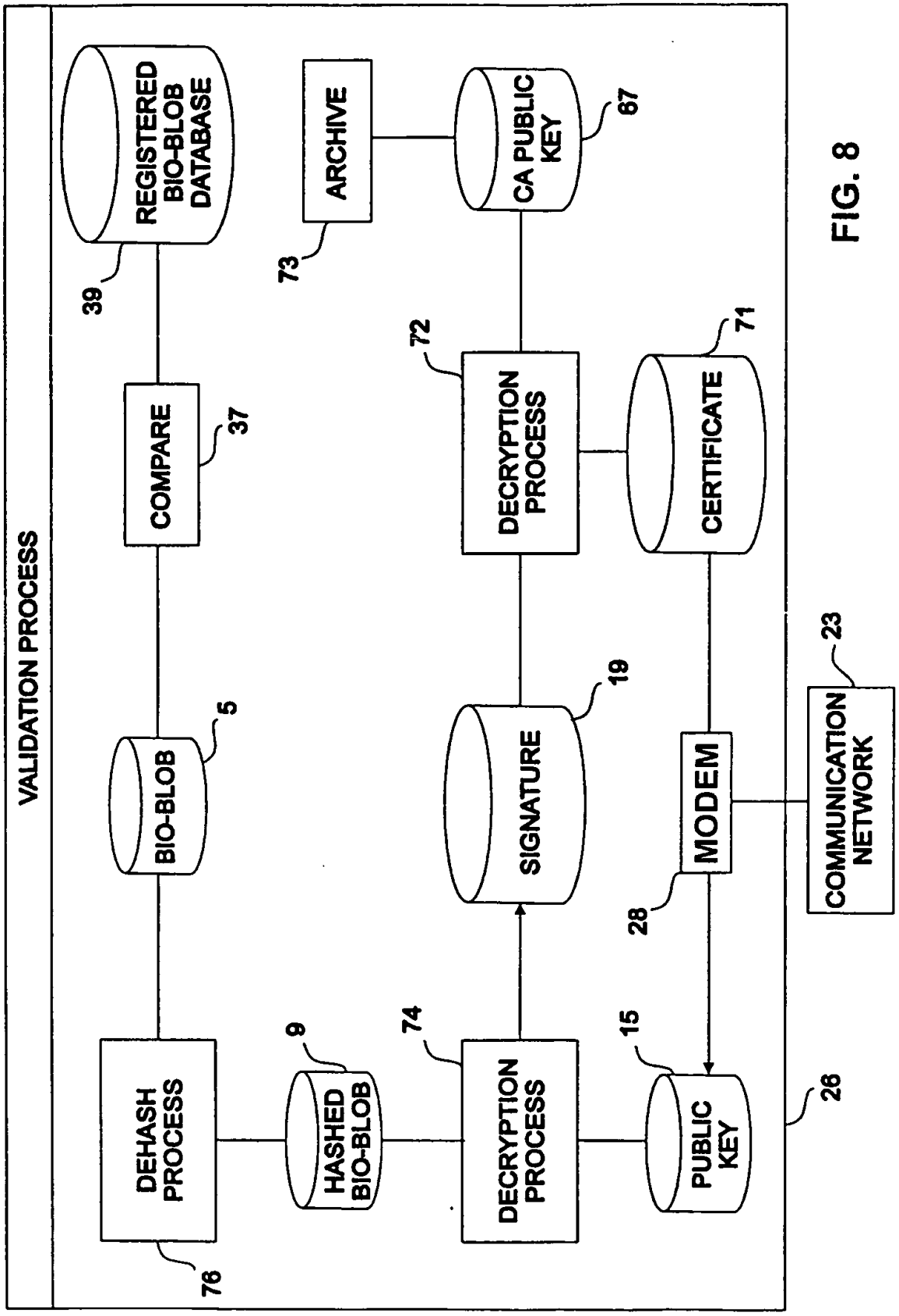

VALIDATION PROCESS
REGISTERED BIO-BLOB DATABASE
39
ARCHIVE
73
CA PUBLIC KEY
67
COMPARE
37
DECRYPTION PROCESS
72
CERTIFICATE
71
BIO-BLOB
5
SIGNATURE
19
MODEM
28
COMMUNICATION NETWORK
23
DEHASH PROCESS
76
HASHED BIO-BLOB
9
DECRYPTION PROCESS
74
PUBLIC KEY
15
26

FIG. 8

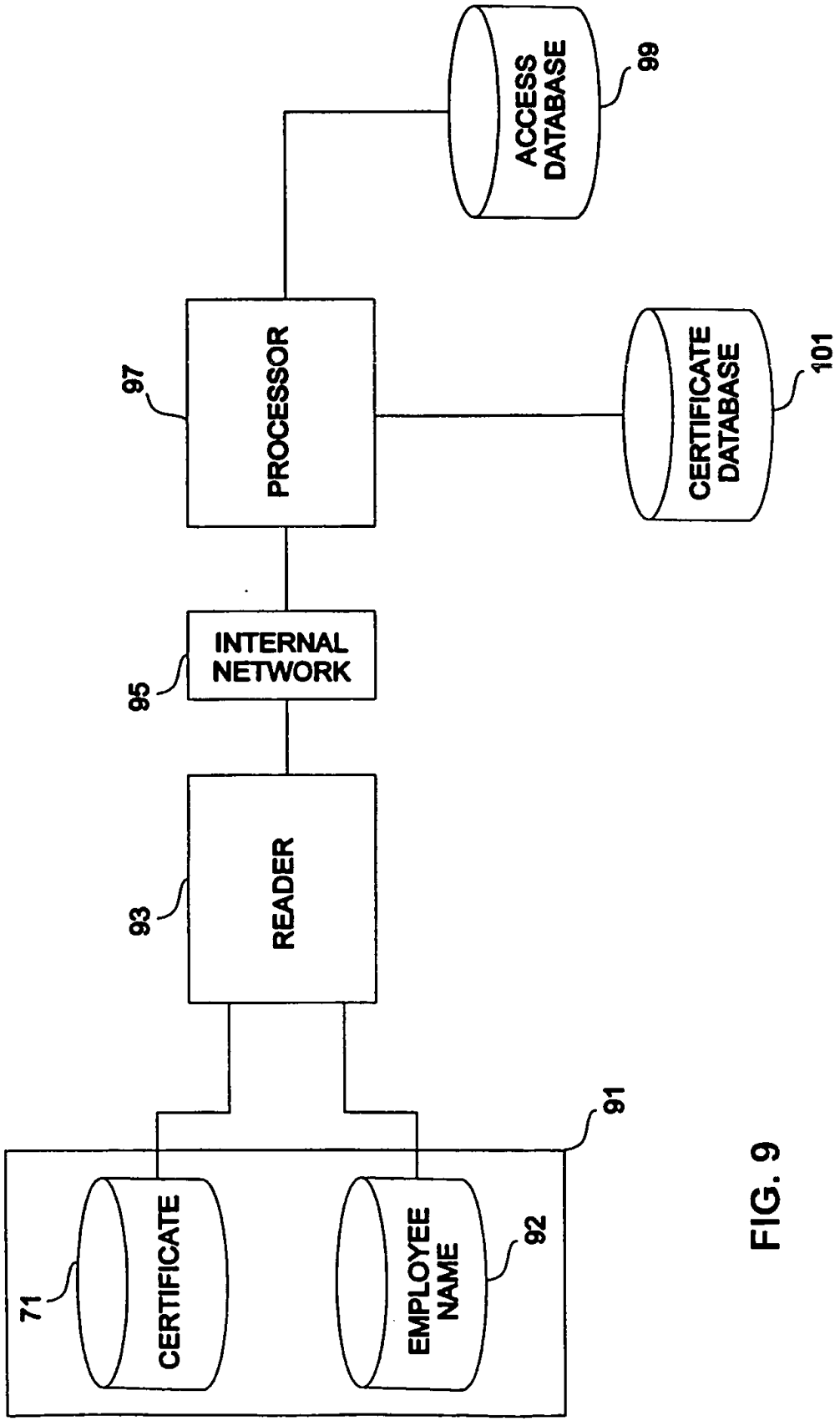

ACCESS DATABASE
99
PROCESSOR
97
CERTIFICATE DATABASE
101
INTERNAL NETWORK
95
READER
93
91
CERTIFICATE
71
EMPLOYEE NAME
92

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/16909

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/32
US CL :713/202

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/202; 380/4, 23, 25, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG, DERWENT, WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 5,872,848 A (ROMNEY et al.) 16 February 1999 (16.02.99), col. 5, lines 1-5, 29-37, col. 6, line 67, col. 7, lines 1-3, 15-67, col. 8, lines 21-33, 47-51 col. 9, lines 29-40, col. 11, lines 26-33, figure 2, steps 220, 275, and 285, figure 9.	5, 8
----		----
Y,P		1-4, 6, 7, 10-17, 21-24, 28, 29, 31-33, 40, 41
Y,P	US 5,917,913 A (WANG) 29 June 1999 (29.06.99), col. 2, lines 56-63, col. 5, lines 65-67, col. 6, lines 1-14, col. 7, lines 1-34, figure 3A, figure 3B, item 354.	1-4, 7, 10-17, 21-24, 28-33, 40, 41
Y,P	US 5,903,882 A (ASAY et al.) 11 May 1999 (11.05.99), col. 2, lines 61-64, col. 14, lines 18-51, col. 15, lines 2-12, 14-20, 27-35.	3, 4, 6, 22-24, 28-33, 41

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 10 SEPTEMBER 1999	Date of mailing of the international search report 22 OCT 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JUSTIN T. DARROW Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/16909

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,208,858 A (VOLLERT et al.) 04 May 1993 (04.05.93), col. 1, lines 7-12, col. 2, lines 3-8.	11
Y	US 5,386,104 A (SIME) 31 January 1995 (31.01.95), col. 1, lines 16-25, col. 4, lines 19-27.	14, 30